

---

# Stichwortverzeichnis

## A

Abbildung  
  logistische, 158

Abbildungsverband  
  gekoppelter, 158

Adressraum, authentifikationsabhängiger  
  virtueller, 105

Advanced Encryption Standard  
  Anforderungen, 148  
  an Anwendungsprogramme, 114  
  an Datendateien, 115

Anforderungsspezifikation, 89

Angreifbarkeit der Prozessorarchitektur,  
  59, 124

Angriff  
  direkter, 24  
  indirekter, 28

Antiheuristikviren, 44

Antivalenz, 149–150, 159, 161

Antivirensoftwarehäuser, 4

Anwender, 4

Aufspüren von Eindringlingen, 18, 68, 70

ausführbare Internetinhalte, 56, 123

Authentifikation, 154, 167  
  Ausweiskartenleseeinheit, 104  
  biometrische Merkmale, 24  
  Gesten oder Tippverhalten, 105  
  Hand- oder Fingerabdrücke, 104  
  persönlicher Besitz, 24  
  Schlüsselschalter, 103  
  sichere mehrseitige, 135  
  spezifisches Wissen, 24

Authentifizierung, 154, 167  
Authentifizierungsverfahren, 18, 24

## B

Basisanforderungen, 90, 127

Befehle, 46, 60, 75, 78–84, 90, 106

Betriebsmittel  
  zu schützende, 93

Betriebssystem, 17, 18, 26, 28, 31–37, 39, 41,  
  42, 45, 47, 48, 50, 53, 58, 59, 67, 80,  
  81, 85, 89, 91, 94–99, 102, 108, 109,  
  123

Bootviren, 33  
  Doppelinfektion, 37  
  Festplatte formatieren, 36  
  Infektion, 35  
  Neuerstellung des MBR, 36  
  Notfallmedien, 36  
  Schreibschutz, 37

Bootvorgang, 34  
  mit Bootvirus, 35  
  ohne Bootvirus, 34

## C

Chaostheorie, 158

CIH-Virus, 32, 36

Cloud, 147, 153

Companion-Viren, 43

## D

Data Encryption Standard, 148

Daten, 82

**Datendateien**

- mit interpretierbarem Code, 116
- ohne interpretierbaren Code, 116

Detailanforderungen, 93

Dropper, 44, 55, 74

Duqu, 59

Durchprobieren, 148, 150

**E**

E-Mail, 17, 39, 41, 57, 126, 153

effektive Lebensdauer, 115

Eindringen

- direktes, 23
- indirektes, 23

Einmalschlüssel

- Erzeugung, 152

Einmalverschlüsselung, 148–155

**F**

Fehlbedienung

- falsche Konfiguration, 119

Fehlerfunktion, 159–160

Fernwartung, 111

Fingered-Angriff, 46

Flame, 59

Funktion des Überwachungssystems, 120

**G**

Geheimtext, 148, 160, 161, 164

gekoppelter Abbildungsverband, 158, 159

Grenzfälle von Malware, 14

grundsätzliche Ansprüche an  
Rechnersysteme, 90

**H**

Harvard-Architektur, 81–84

- Emulation, 84

Hashfunktion, 99, 101, 102

Herzschrittmacher, 147

heuristische Suche, 70

Hintertüren, 44, 55

Hoaxes, 14

homophone Substitution, 161, 162

hybride Viren, 45

**I**

Impfen mit Virensignaturen, 69

Industrie 4.0, 153

Integrität, 14, 17

Integritätsprüfung, 70, 71, 74

intelligentes Stromnetz, 154

Internet der Dinge, 61, 153

Internet-Banking, 167

Internet-Wurm, 45

IRC (Internet Relay Chat), 50

I love you-Wurm, 16, 41, 47

- Ausbreitungsarten, 53
- Auswirkungen, 15, 20
- Erfolgsanalyse, 54
- Schadensfunktionen, 47
- Varianten, 54

**K**

Kerckhoffssches Prinzip, 147

Kettenbriefe, 14

Klartext, 19, 114, 147–150

Kommunikationsüberwachung mittels  
Hardware, 73

kontextsensitive Speicherzuordnung, 99

**L**

Lösung ohne Offenbarungsinformation, 119

logische Bomben, 55

logistische Abbildung, 158

**M**

Makroviren, 5, 38

- Bausätze, 40

Malware, 1–7, 13, 14, 16, 18, 67, 77, 80

Meldown, 124

Michelangelo-Virus, 37

Monitorprogramm, 72

Motivation, 1

Multiapplikationsmakroviren, 40

multipartite Viren, 45

**N**

Nächste-Nachbarn-Kopplung, 158

Netzschnittstelle, 85

neue Qualität der Bedrohung, 56

**O**

offenbarendes Verfahren, 111

Offenbarungsdatei

Muster, 117

**P**

perfekte kryptographische Sicherheit, 148

polymorphe Viren, 33, 39, 43

Programmauthentifizierung, 73, 81, 89

Programmtechnik, 42

programmunbeeinflussbare Schutzmaßnahmen,  
89

Programmverschlüsselung, 45, 81

Programmviren, 31

Pseudozufallsbits, 157, 158, 166, 167

psychologische Aspekte, 61

**R**

Reaktionen auf unerlaubte Aktionen, 123

rechtliche Grundlagen, 8–13

Ausspähen von Daten, 8

Betrug, 9

Computerbetrug, 10

Computersabotage, 12

Datenveränderung, 12

Erschleichen von Leistungen, 10

Fälschung beweisbarer Daten, 11

Fälschung technischer Aufzeichnungen, 11

Sachbeschädigung, 11

Strafantrag, 12

Täuschung im Rechtsverkehr bei

Datenverarbeitung, 11

Urkundenfälschung, 10

Relation, 162, 163, 165

Remote Shell-Angriff, 46

Restrisiko, 126

Retroviren, 44

Robustheit, 93, 127

Roter Oktober, 57

RSA-Verfahren, 148

**S**

Schlüssel, 148

Schnittstellenanalyse, 68

Schreibschutzkopplung gerätetechnische, 102

Schutzmaßnahmen

präventive, 68

Schutzziele, 17

Sendmail-Angriff, 46

Shannon, C. E., 148

sichere Eingabe für mobile Geräte, 131

sichere mehrseitige Authentifikation, 135

Sicherheitsbereich, 24, 91, 92, 95–97, 101

Sicherung mobiler Geräte, 131

Softwarefunktionen

sicherheitsrelevante, 94

Softwarelösung, 80

Spectre, 59, 124

Speicherüberwachung mittels Hardware, 73

Speichersegmentierung, 95

Stealth-Viren, 42

Stellvertreterviren, 43

Stromverschlüsselung, 158, 159

Stuxnet, 58

**T**

Tarnkappenviren, 42

Tremor-Virus, 32

Trojanisches Pferd, 55

tunnelnde Viren, 44

**U**

Überflutungsangriff, 2, 7, 74, 94, 127

Überwachungssystem Funktion, 120

Unangreifbarkeit, 90, 102

Unterbrechungsüberwachung mittels  
Hardware, 72

**V**

Verbindlichkeit, 17

Verfügbarkeit, 17

Vernam, 151

Verschlüsselung, 147, 165

Verschlüsselungsgerät, 163

Verschleierung, 157, 161, 165

vertraulicher Kanal, 148, 165, 167

Vertraulichkeit, 14, 17, 127, 137, 167

Viren, 28

Aufbau, 28

Auslösebedingung, 30

Viren (*Fort.*)

- Begriffserklärung, 29
- Infektion, 29
  - speicherresidente, 30
  - unmittelbare, 29
- Infektionsteil, 29
  - polymorphe, 32, 39, 43
  - tunnelnde, 44
- Schadensteil, 29, 31
- Virensignatur, 28
- Virenprogrammierer, 3
- Virensignatur, 28, 29, 37, 44
- Virensignatursuche, 33, 42, 70

- von Neumann-Architektur, 18, 77
- vorbeugende Maßnahmen, 68

**W**

- Würmer, 45
- Warnmeldung, 14, 68
- Wirtsprogramme, 28–31

**Z**

- Zeitbombe, 55